DEPARTMENT OF THE NAVY
NAVY ENVIRONMENTAL HEALTH CENTER
2510 WALMER AVENUE
NORFOLK, VIRGINIA 23513-2617

NAVENVIRHLTHCENINST 3070.1
OO:RJ
19 APR 1995

NAVENVIRHLTHCEN INSTRUCTION 3070.1

From: Commanding Officer, Navy Environmental Health Center

Subj: OPERATIONS SECURITY

Ref: (a) OPNAVINST 3070.1A

Encl: (1) Command OPSEC Plan

1. Purpose

a. To provide local guidance supporting reference (a) and assign responsibility and direct planning actions to protect essential secrecy of unclassified, yet critical mission elements, which may serve as indicators of friendly intentions, naval capabilities and current activities of foreign intelligence collection operatives.

b. To publish the Command OPSEC Plan, (Enclosure (1)).

2. Definition. Operations Security (OPSEC) is the process of analyzing friendly actions attendant to military operations and other activities to:

a. Identify actions that can be observed by hostile intelligence systems.

b. Determine indicators the hostile intelligence system might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate, or reduce to an acceptable level, vulnerabilities of friendly actions to hostile exploitation.

3. Background. The intelligence threat to U.S. military operations and activities today is formidable and continues to grow. Potential adversaries are actively working to gain information about our capabilities and limitations, intentions and plans, and tactics and readiness. They find valuable sources of exploitable information in communications patterns, stereotyped procedures, and many types of unclassified information. These sources are outside the purview of traditional security programs (e.g. Information Security, Physical Security) and are often overlooked as potential security

breaches. The OPSEC program, as defined in reference (a), is designed to deal with these issues. Whereas traditional security programs deal with only part of the information disclosure program, the OPSEC program addresses the total problem, including unclassified, but sensitive, information. Protective measures duplicating those of traditional security programs, however, are not the principal concern of OPSEC.

4. Policy. Because even simple, routine activities can involve serious OPSEC weaknesses, OPSEC considerations need to be integrated fully into all daily duties, as well as military operations. This includes an awareness of command or supported command, intentions, capabilities, and activities that might be of potential interest to adversaries under various circumstances. OPSEC is the responsibility of all hands. As such, adhere to the following:

a. Make maximum use made of the Secure Telephone Unit III (STU III) when discussing unclassified, yet sensitive, information.

b. Shred hard copy unclassified, but sensitive, information.

5. Training

a. Train all newly reported personnel concerning local OPSEC threats and procedures within 60 days of reporting.

b. Conduct annual follow-on training for all personnel.

6. Responsibilities

a. The Commanding Officer is responsible for ensuring that training, planning and specific actions are undertaken which enhance the essential secrecy of operational elements, which if otherwise revealed, could, deter the effectiveness of the command or other supported units' accomplishing their mission.

b. Security Manager

(1) Prepare and review general OPSEC planning instructions.

(2) Identify, in consultation with the Public Affairs Officer (PAO), Essential Elements of Friendly Information which may be considered for specific OPSEC application measures.

(3) Conduct an ongoing OPSEC awareness program.

(4) Ensure the continuous viability of other supporting security programs such as Information, Personnel, Physical and Automated Information Systems Security.

c. <u>Training Officer</u>. Sponsor and monitor accomplishment of staff OPSEC training.

7. <u>Action</u> This plan is effective upon receipt for planning and operations in support of OPSEC.

P. D. BARRY

Distribution: (NAVENVIRHLTHCENINST 5215.2N)

List V	(All Staff Personnel)
List VI	(NAVENPVENTMEDUs)
List VII	(NAVDISVECTECOLCONCENs)
List VIII	(NAVENVIRHLTHCEN DETs)
List IX	(NAVDRUGLABs)

COMMAND OPSEC PLAN

1. Purpose. To provide specific planning guidance for implementing an OPSEC program at NAVENVIRHLTHCEN, Norfolk, VA.

2. Threats. There are several types of threats faced by the command where OPSEC measures may be of value.

a. Theft. Hostile intelligence organizations, disaffected personnel, and criminals observe physical security practices to find vulnerabilities they can exploit to steal documents of values.

b. Personnel Subornment. Hostile intelligence organizations and criminals gather data about personnel to detect access to matters of interest in personnel character, indebtedness, and other vulnerabilities. Thus the OPSEC practices of individuals, personnel offices, finance offices and others who deal with personnel records must be such as to keep secret indicators that could be used by adversaries.

c. Terrorism. The command must ensure command personnel are aware of, and, when a terrorist intent and capability is present, use OPSEC measures to reduce vulnerabilities to attack.

d. Inadvertent Disclosures. Inadvertent introducing open sources indicators by statements, press releases, conversations, articles, letters, and other actions. Hostile intelligence services train personnel in techniques for eliciting information during conversations, frequenting areas where government employees congregate, gathering base newspapers, Plans of the Day, telephone books, organizational manuals, technical manuals, and other such data. The command must ensure personnel are aware of the questions hostile intelligence attempt to answer and of the potential indicators they must protect.

3. Structure. The Command Security Officer has primary responsibility for implementing the OPSEC program. Other elements having significant OPSEC responsibilities are the Fleet Liaison Officer, ADP Security Officer, Materials Management Department, Plans and Operations Officer, and Personnel Management staff.

4. Training

a. Provide OPSEC training to newly reporting personnel within 60 days of reporting to or being hired by the command.

b. Implement a continuing awareness campaign through annual refresher training in OPSEC and counter terrorism, posters, Plan of the Week notes, discussions of specific concerns, etc.

c. Provide individuals in key assignments additional OPSEC planning skills, preceding and during the execution of sensitive operations or support missions. Consider external resources (i.e., Naval Criminal Investigative Service, Base Security, etc.) to assist in this training.